ALIBABA CLOUD

Alibaba Cloud

PrivateLink
User Guide

Document Version: 20220616

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

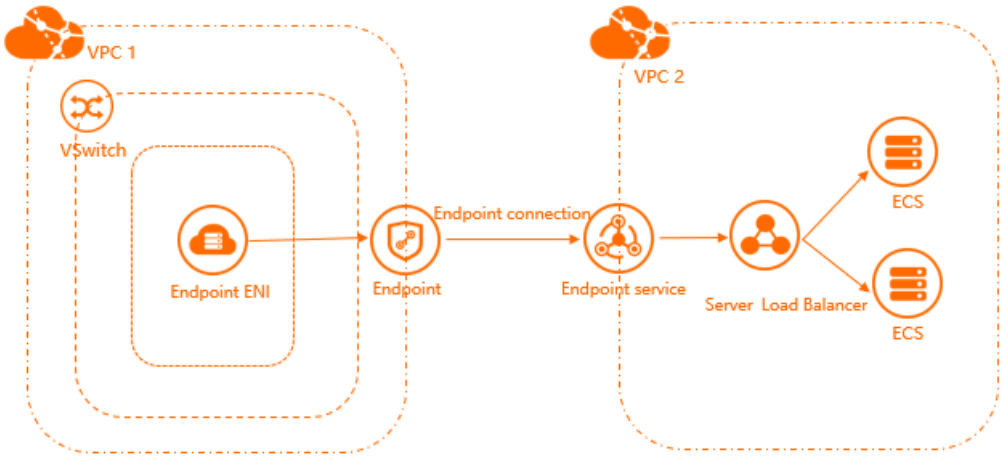
1.Endpoints

1.1. Endpoint overview

This topic provides an overview of endpoints, and describes how to create an endpoint and use the endpoint to access an endpoint service.

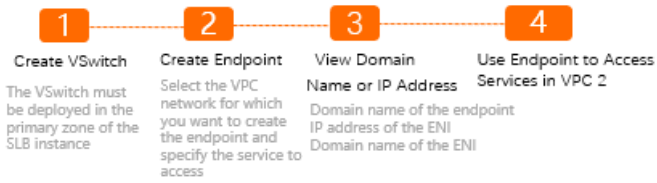
Overview

You can associate an endpoint in a virtual private cloud (VPC1) with an endpoint service in another VPC (VPC2). This way, VPC1 can access the Server Load Balancer (SLB) instance in VPC2. Endpoints are created and managed by service consumers.



Procedure

Perform the following operations to create an endpoint and use the endpoint to access an endpoint service:



1. Create a vSwitch

   Create a vSwitch. Make sure that the vSwitch is deployed in the primary zone of the SLB instance that serves as the service resource. After the vSwitch is created, the system creates an endpoint elastic network interface (ENI) in the vSwitch. The endpoint ENI serves as an ingress for the VPC in which the endpoint is deployed to access the endpoint service.

2. Create an endpoint

   Create an endpoint and associate the endpoint with the endpoint service. This way, the VPC in which the endpoint is deployed can access the SLB instance in the VPC in which the endpoint service is deployed. For more information, see Create an endpoint.

3. View the domain name and IP address that can be used to access the endpoint service

   After the endpoint is created, you can view the domain name and IP address that can be used to access the endpoint service. For more information, see View the domain name and IP address that

can be used to access the endpoint service.

4. Access the endpoint service

   Access the endpoint service by using the domain name of the endpoint, the domain name of the zone in which the endpoint is deployed, or the IP address.

1.2. Create and manage endpoints

This topic describes how to create and manage endpoints. You can associate endpoints with endpoint services. This way, you can establish PrivateLink connections between virtual private clouds (VPCs) and other Alibaba Cloud services.

Background information

PrivateLink allows you to establish secure, stable, and private connections between VPCs and other Alibaba Cloud services. Compared with connections over the Internet, PrivateLink provides higher security. You can create an endpoint and associate the endpoint with an endpoint service. This way, you can establish PrivateLink connections between a VPC and other Alibaba Cloud services.

Limits

PrivateLink is available for use only in specific regions. For more information, see Regions and zones that support PrivateLink.

Operations

- Create an endpoint
- View the domain name or IP address that can be used to access an endpoint service
- Modify an endpoint
- Delete an endpoint

Prerequisites

Before you create an endpoint, make sure that the following requirements are met:

- If this is your first time using PrivateLink, log on to the Activation page to activate PrivateLink.
- An endpoint service is created and at least one service resource is added to the endpoint service. For more information, see 创建和管理终端节点服务.
- A VPC that is used to access the endpoint service is created. A vSwitch is created in the zone in which the endpoint service is created. For more information, see Create a VPC and a vSwitch.
- A security group is created.
  - If you create an endpoint whose **Endpoint Type** parameter is set to **Interface Endpoint**, you can configure security group rules based on your business and security requirements. We recommend that you configure the following security group rules:
    - A default rule that supports Internet Control Message Protocol (ICMP) for operations such as pinging the ECS instance.
    - A default inbound rule that allows traffic on SSH port 22 and Remote Desktop Protocol (RDP) port 3389 to access the ECS instance.
    - Optional. An inbound rule that allows traffic on HTTP port 80 and HTTPS port 443. This rule allows the VPC of the endpoint to access the VPC of the endpoint service over HTTP or HTTPS.

- If you create an endpoint whose **Endpoint Type** parameter is set to **Reverse Endpoint**, you must configure an inbound rule that **allows all traffic**. This means that you must allow all CIDR blocks to access all ports over all protocols.

For more information, see Create a security group.

Create an endpoint

1.
2. In the top navigation bar, select the region where you want to create an endpoint.
3. On the **Endpoints** page, you can use one of the following methods to create an endpoint:
   - Click the **Interface Endpoint** tab, and then click **Create Endpoint**.
   - Click the **Reverse Endpoint** tab, and then click **Create Endpoint**.

   > **Note**
   > - An interface endpoint allows the service consumer to access the service that is provided by the service provider. A reverse endpoint allows the service provider to access resources in the VPC of the service consumer.
   > - Endpoints are created and managed by service consumers. Endpoint services are created and managed by service providers.

4. On the **Create Endpoint** page, set the following parameters and click **OK**.

Parameter	Description
Endpoint Name	Enter a name for the endpoint. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). The name must start with a letter.
Endpoint Type	Select an endpoint type. Valid values: - **Interface Endpoint**: An interface endpoint allows the service consumer to access the service that is provided by the service provider. - **Reverse Endpoint**: A reverse endpoint allows the service provider to access resources in the VPC of the service consumer.
Endpoints Service	You can associate an endpoint with an endpoint service by using one of the following methods: - Click **Add by Service Name** and enter an endpoint service name. - Click **Select Service** and select the ID of the endpoint service. **Note** You can associate an endpoint with only one endpoint service.
VPC	Select the VPC where you want to create the endpoint.

Parameter	Description
Security Groups	Select the security group to be associated with the endpoint elastic network interface (ENI). The security group is used to control data transfer from the VPC to the endpoint ENI. **Note** Endpoint ENIs serve as entries for VPCs to access endpoint services.
Zone and vSwitch	Select the zone of the endpoint service and select a vSwitch in the zone. The system automatically creates an endpoint ENI in the vSwitch.
Description	Enter a description for the endpoint. The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`.
Note	When you create an endpoint for the first time, the system automatically creates a service-linked role for PrivateLink. The role allows the endpoint to access other resources. For more information, see Service linked role.

View the domain name or IP address that can be used to access an endpoint service

After you create an interface endpoint, you can use the domain name of the endpoint, the domain name of the zone in which the endpoint is created, or an IP address to access the service resources of the endpoint service.

1.
2. In the top navigation bar, select the region where the endpoint is created.
3. On the **Endpoints** page, click the **Interface Endpoint** tab.
4. On the **Interface Endpoint** tab, find the endpoint that you want to manage and click its ID.
5. On the details page of the endpoint, you can view the domain name of the endpoint, the domain name of the zone in which the endpoint is created, and the IP address. You can use the domain names and the IP address to access the endpoint service.

Note If you create a reverse endpoint, PrivateLink does not provide the domain name of the endpoint or the domain name of the zone in which the endpoint is created.

Modify an endpoint

You can modify the name and description of an endpoint.

1.
2. In the top navigation bar, select the region where the endpoint is created.
3. On the **Endpoints** page, click the **Interface Endpoint** tab or the **Reverse Endpoint** tab, find the

endpoint that you want to manage and click its ID.

- To modify the name of an endpoint, perform the following steps:
  a. In the **Information** section, click **Edit** next to **Instance Name**.
  b. In the dialog box that appears, enter a new name and click **OK**.

     The name must be 2 to 100 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). The name must start with a letter.
- To modify the description of an endpoint, perform the following steps:
  a. In the **Information** section, click **Edit** next to **Description**.
  b. In the dialog box that appears, enter a new description and click **OK**.

     The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`.

Delete an endpoint

You can delete an endpoint that you no longer need. After you delete an endpoint, the VPC in which the endpoint is deployed cannot access endpoint services through PrivateLink.

> **Note** Before you delete an endpoint, you must delete the ENI that is associated with the endpoint. For more information, see Delete the ENI of an endpoint.

1.
2. In the top navigation bar, select the region where the endpoint is created.
3. On the **Endpoints** page, click the **Interface Endpoint** tab or the **Reverse Endpoint** tab, find the endpoint that you want to delete and click **Delete** in the **Actions** column.
4. In the **Delete Endpoint** message, click **OK**.

References

- CreateVpcEndpoint: creates an endpoint.
- ListVpcEndpoints: queries endpoints.
- UpdateVpcEndpointAttribute: modifies an endpoint.
- DeleteVpcEndpoint: deletes an endpoint.

1.3. Manage security groups

After you create an endpoint for a virtual private cloud (VPC), you can add the endpoint to a security group. This way, you can manage the traffic between the VPC and the endpoint elastic network interface (ENI). If you no longer need a security group, you can remove the endpoint from the security group.

Operations

- Add an endpoint to a security group
- Remove an endpoint from a security group

Prerequisites

- An endpoint is created. For more information, see Create and manage endpoints.
- At least two security groups are created in the VPC of the endpoint, and the security group rules meet the following requirements:
  - If you create an endpoint whose **Endpoint Type** parameter is set to **Interface Endpoint**, you can configure security group rules based on your business and security requirements. We recommend that you configure the following security group rules:
    - A default rule that supports Internet Control Message Protocol (ICMP) for operations such as pinging the ECS instance.
    - A default inbound rule that allows traffic on SSH port 22 and Remote Desktop Protocol (RDP) port 3389 to access the ECS instance.
    - Optional. An inbound rule that allows traffic on HTTP port 80 and HTTPS port 443. This rule allows the VPC of the endpoint to access the VPC of the endpoint service over HTTP or HTTPS.
  - If you create an endpoint whose **Endpoint Type** parameter is set to **Reverse Endpoint**, you must configure an inbound rule that **allows all traffic**. This means that you must allow all CIDR blocks to access all ports over all protocols.

  For more information, see Create a security group.

Add an endpoint to a security group

1.
2. In the top navigation bar, select the region where the endpoint is deployed.
3. On the **Endpoints** page, click the **Interface Endpoint** or **Reverse Endpoint** tab, find the endpoint that you want to manage and click its ID.
4. On the details page of the endpoint, click the **Security Group** tab, and then click **Join Security Group**.
5. In the **Join Security Group** dialog box, select a security group and click **OK**.

Remove an endpoint from a security group

Before you remove an endpoint from a security group, make sure that the endpoint is added to at least one security group.

1.
2. In the top navigation bar, select the region where the endpoint is deployed.
3. On the **Endpoints** page, click the **Interface Endpoint** or **Reverse Endpoint** tab, find the endpoint that you want to manage and click its ID.
4. On the details page of the endpoint, click the **Security Group** tab, find the security group that you want to manage, and then click **Delete** in the **Actions** column.
5. In the **Remove Security Group** message, click **OK**.

References

- AttachSecurityGroupToVpcEndpoint: adds an endpoint to a security group.
- DetachSecurityGroupFromVpcEndpoint: removes an endpoint from a security group.

1.4. Create and manage endpoint ENIs

An endpoint elastic network interface (ENI) serves as an ingress for the virtual private cloud (VPC) in which the endpoint is deployed. The VPC can use the endpoint ENI to access the associated endpoint service. After you create an endpoint ENI, you can use the private IP address of the ENI or the domain name of the endpoint to access the endpoint service. You can also delete an endpoint ENI that you no longer need.

Operations

- Create an endpoint ENI
- Delete an endpoint ENI

Prerequisites

An endpoint is created. For more information, see Create and manage endpoints.

Create an endpoint ENI

When you create an endpoint ENI, make sure that a service resource of the endpoint service is deployed in the zone that you select. Make sure that a vSwitch is created in the zone. For more information, see Create a vSwitch.

1.
2. In the top navigation bar, select the region where the endpoint is deployed.
3. On the **Endpoints** page, click the **Interface Endpoint** or **Reverse Endpoint** tab, find the endpoint that you want to manage and click its ID.
4. On the endpoint details page, click the **Zone and ENI** tab, and then click **Add Zone**.
5. In the **Add Zone** dialog box, select the zone and the vSwitch to which the endpoint ENI belongs, and click **OK**.

Delete an endpoint ENI

1.
2. In the top navigation bar, select the region where the endpoint is deployed.
3. On the **Endpoints** page, click the **Interface Endpoint** or **Reverse Endpoint** tab, find the endpoint that you want to manage and click its ID.
4. On the endpoint details page, click the **Zone and ENI** tab. Find the endpoint ENI that you want to delete and click **Delete** in the **Actions** column.
5. In the **Remove Zone** message, click **OK**.

References

- AddZoneToVpcEndpoint: adds a zone for an endpoint.
- RemoveZoneFromVpcEndpoint: deletes a zone of an endpoint.

2.Endpoint services

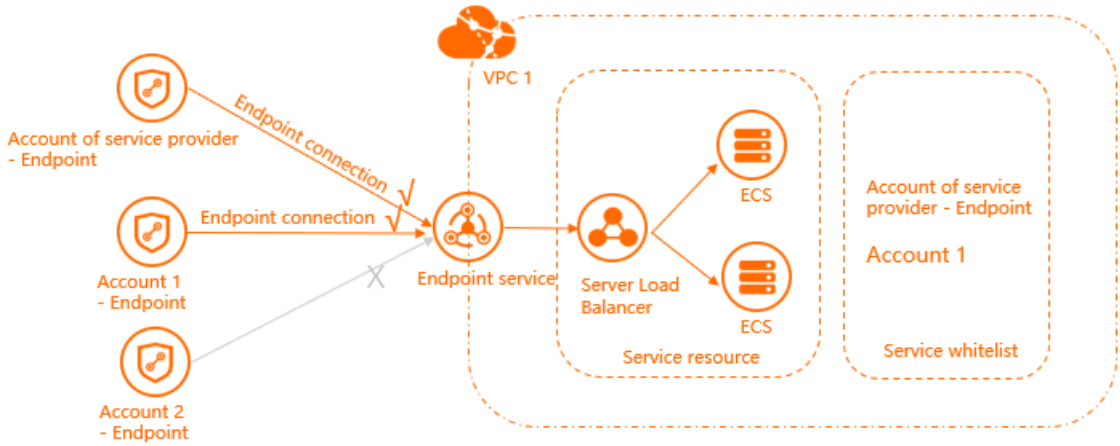
2.1. Overview of endpoint services

This topic introduces endpoint services and describes how to create an endpoint service.

Note

Overview

You can use an endpoint in a virtual private cloud (VPC) to connect to an endpoint service that is deployed in another VPC through PrivateLink. Endpoint services are created and managed by service providers.



Procedure

The following flowchart shows how to create an endpoint service.

1. Create an internal Server Load Balancer (SLB) instance that supports the PrivateLink service

   Only internal SLB instances that support the PrivateLink service can serve as service resources for endpoint services. You must specify SLB instances as service resources when you create an endpoint service. Before you create an endpoint service, you must create an internal SLB instance that supports the PrivateLink service. For more information, see 创建和管理终端节点服务.

2. Configure the SLB instance

   After the SLB instance is created, you must add at least one listener and one group of backend servers to the SLB instance. This way, traffic can be forwarded by the SLB instance. For more information, see Configure a CLB instance.

3. Create an endpoint service

   You can use an endpoint in a VPC to connect to an endpoint service that is deployed in another

VPC through PrivateLink. You must specify SLB instances when you create an endpoint service. For more information, see Create endpoint services.

4. Add account IDs to the whitelist

   After you create an endpoint service, the account ID of the service owner is automatically added to the whitelist. The endpoint service is visible to users whose account IDs are in the whitelist. These users can use the endpoints to connect to the endpoint service. To allow VPCs under other accounts to access endpoint services deployed in your VPC, you must add their account IDs to the whitelist. For more information, see Manage account IDs in the whitelist.

5. Optional. Add service resources to an endpoint service.

   You can add multiple service resources to an endpoint service. After you create an endpoint in a VPC, you can use the endpoint to access the endpoint services that are deployed in another VPC through PrivateLink. For more information, see Add and remove service resources.

2.2. Manage endpoint services

2.2.1. Create endpoint services

This topic describes how to create endpoint services. You can create an endpoint service in your virtual private cloud (VPC) and allow other VPCs to access the endpoint service.

Prerequisites

Make sure that the following requirements are met:

-
- If this is your first time using PrivateLink, log on to the Activation page to enable PrivateLink.
- A Classic Load Balancer (CLB) instance that supports PrivateLink is created. For more information, see 创建和管理终端节点服务.

Procedure

1. Log on to the Endpoints Service console.
2. In the top navigation bar, select the region where you want to create an endpoint service.
3. On the **Endpoints Service** page, click **Create Endpoint Service**.
4. On the **Create Endpoint Service** page, set the following parameters and click **OK** to create an endpoint service.

Parameter	Description
Select Service Resource	Select a zone to distribute network traffic. Then, select the CLB instance to be associated with the endpoint service. If you do not have a CLB instance that supports PrivateLink, see Create a CLB instance. Go to the buy page of CLB and create a CLB instance that supports PrivateLink. You can click **Add Resource from Another Zone** to add multiple service resources.

Parameter	Description
Automatically Accept Endpoint Connections	Specify whether to automatically accept connection requests from an endpoint. ○ **Yes**: The endpoint service accepts all connection requests from the associated endpoint. If you select this option, you can use the associated endpoint to directly access the endpoint service. ○ **No**: If you select this option, the newly created endpoint service is in the **Disconnected** state. The service administrator must manually accept or deny connection requests. ■ If the service administrator accepts endpoint connection requests from the associated endpoint, you can use the endpoint to access the endpoint service. ■ If the service administrator denies endpoint connection requests from the associated endpoint, the endpoint service cannot be accessed through the endpoint.
Whether to Enable Zone Affinity	Select whether to enable zone affinity: ○ If you select **Yes**, the endpoint service preferentially accepts requests from endpoints in the same zone. ○ If you select **No**, the endpoint service does not preferentially accept requests from endpoints in the same zone.
Description	Enter a description for the endpoint service. The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`.

Related information

- CreateVpcEndpointService

2.2.2. Modify endpoint services

This topic describes how to modify endpoint services. You can change the description and default maximum bandwidth, and specify whether to automatically accept connection requests from endpoints.

Procedure

1.
2.
3. In the top navigation bar, select the region where the endpoint service is deployed.
4. On the **Endpoint Service** page, click the service ID of the endpoint service that you want to modify.
5. In the **Information** section, perform the following operations to modify the endpoint service:
   - Specify whether to automatically accept endpoint connections

Click **Enable** or **Disable** next to **Automatically Accept Endpoint Connections**, and then click **OK** in the message that appears.

- Modify the description

  Click **Edit** next to **Description**. In the dialog box that appears, enter a new description, and click **OK**.

  The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`.

- Modify the default maximum bandwidth

  Click **Modify** next to **Default Maximum Bandwidth**. In the **Change Bandwidth** dialog box, specify a new bandwidth value, and then click **OK**.

Related information

- UpdateVpcEndpointAttribute

2.2.3. Delete an endpoint service

This topic describes how to delete endpoint services. After you delete an endpoint service, the Server Load Balancer (SLB) instances that are associated with the endpoint service are still retained.

Prerequisites

Before you create an endpoint service, make sure that the following requirements are met:

- Endpoints that are associated with the endpoint service are in the rejected state. For more information, see Reject endpoint connection requests.
- Service resources that are added to the endpoint service are removed. For more information, see Remove service resources.

Procedure

1.
2.
3. In the top navigation bar, select the region where the endpoint service is deployed.
4. On the **Endpoint Service** tab, find the endpoint service from which you want to remove service resources, and click **Delete** in the **Actions** column.
5. In the dialog box that appears, click **OK**.

Related information

- DeleteVpcEndpointService

2.3. Manage service resources

2.3.1. Add and remove service resources

After you create an endpoint service, you can add service resources to the endpoint service. After an endpoint connection is established between the endpoint of a virtual private cloud (VPC) and the endpoint service, the VPC can access the service resources of the endpoint service through PrivateLink. You can also remove the service resources that you no longer need from the endpoint service.

Operations

- Add service resources
- Remove a service resource

Add service resources

1. Log on to the Endpoint Service console.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, find and click the endpoint service that you want to manage.
4. On the details page of the endpoint service, click the **Service Resources** tab, and then click **Add Service Resource**.
5. In the **Add Service Resource** dialog box, select the zone to which you want to distribute traffic, add a service resource by using one of the following methods, and then click **OK**.
   - If a service resource is deployed in the zone, you can select the service resource from the drop-down list.
   - If no service resource is deployed in the zone, you can click the drop-down list and create a service resource.

     For more information about how to create a service resource, see Create an SLB instance that supports PrivateLink.

> **Note** If you want to add service resources in different zones, you can click **+ Add Resource from Another Zone**.

Remove a service resource

1.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, click the ID of the endpoint service that you want to manage.
4. On the endpoint service details page, click the **Service Resources** tab, find the service resource that you want to delete, and perform operations based on the following scenarios:
   - If a service resource is not allocated to a zone of an endpoint:
     a. Find the service resource that you want to delete and click **Delete** in the **Actions** column.
     b. In the **Remove Resource** message, click **OK**.
   - If a service resource is allocated to a zone of an endpoint:
     a. Find the service resource that you want to delete and click **Replace Resource** in the **Actions** column.

b. In the **Replace Service Resource** dialog box, set the following parameters and click **OK**.

Parameter	Description
Migration Type	Select **Smooth Migration** or **Forcible Migration** based on your business requirements. ■ If you select **Smooth Migration**, click **Release Previous Endpoint Connections** in the **Actions** after the migration is completed. After the previous connections are released, delete the service resource. ■ If you select **Forcible Migration**, you can directly delete the service resource after the migration is completed.
Select Destination Service Resource	Select the service resource that is used to replace the current service resource.
Select Source Endpoint Connection	Select the endpoint connection that is associated with the current service resource.

c. Find the service resource that you want to delete and click **Delete** in the **Actions** column.

d. In the **Remove Resource** message, click **OK**.

> **Note** If the service resource that you want to delete is allocated to a zone of an endpoint, you must turn off the **Enabled** switch in the **Automatic Allocation** column of the service resource on the **Service Resources** tab.

References

- AttachResourceToVpcEndpointService: adds a service resource to an endpoint service.
- DetachResourceFromVpcEndpointService: removes a service resource from an endpoint service.

2.3.2. Remove service resources

This topic describes how to remove service resources that you no longer need from endpoint services.

Prerequisites

Before you remove a service resource, you must reject connection requests from the endpoint that is associated with the endpoint service. For more information, see Reject endpoint connection requests.

Procedure

1.
2.
3. In the top navigation bar, select the region where the endpoint service is deployed.
4. On the **Endpoint Service** page, find the endpoint service from which you want to remove resources, and click the service ID of the endpoint service.

5. On the **Service Resources** tab, find the service resource that you want to remove, and click **Delete** in the **Actions** column.
6. In the message that appears, click **OK**.

Related information

- DetachResourceFromVpcEndpointService

2.4. Manage endpoint connection requests

2.4.1. Accept endpoint connection requests and manage endpoint connections

You can configure an endpoint service to automatically accept endpoint connection requests. You can also manually accept endpoint connection requests to an endpoint service. After the requests are accepted, endpoint connections are established. You can reject endpoint connection requests based on your business requirements.

Context

When you create an endpoint, you must associate the endpoint with an endpoint service. The endpoint can access the endpoint service only after the endpoint service accepts the connection request from the endpoint. You can specify whether endpoint connection requests are accepted automatically or manually. You can also modify the maximum bandwidth of an endpoint connection or reject endpoint connection requests.

- Specify whether to automatically accept endpoint connections
- Manually accept connection requests
- Modify the maximum bandwidth of an endpoint connection
- Reject endpoint connection requests

Prerequisites

- An endpoint is created. For more information, see Create an endpoint.
- An endpoint service is created.

Specify whether to automatically accept endpoint connections

You can specify whether an endpoint service automatically accepts connection requests based on your business requirements. If an endpoint service is set to automatically accept endpoint connection requests, the endpoint service automatically accepts connection requests from endpoints.

1. Log on to the Endpoint Service console.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, find and click the ID of the endpoint service that you want to manage.
4. In the **Information** section of the details page, click **Enable** or **Disable** next to **Whether to Automatically Accept Connections**.

- **Enable**: After you create an endpoint that is associated with the endpoint service, the endpoint service automatically accepts the connection request from the endpoint. You can use the endpoint to access the service resources of the endpoint service.
- **Disable**: After you create an endpoint that is associated with the endpoint service, the endpoint connection is in the **Disconnected** state. You cannot use the endpoint to access the service resources of the endpoint service.

5. In the message that appears, click **OK**.

Manually accept connection requests

If an endpoint service is not configured to automatically accept endpoint connection requests, you must manually accept endpoint connection requests. After endpoint connection requests are accepted, the associated endpoints can access the service resources of the endpoint service over PrivateLink connections.

Before you accept a connection request, make sure that the following requirements are met:

1. The endpoint connection is in the **Disconnected** state.
2. The zone of the endpoint is in the **Pending to Be Connected** or **Disconnected** state.

After you accept the connection request from an endpoint, the status of the endpoint connection changes to **Connected**.

1. Log on to the Endpoint Service console.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, find and click the ID of the endpoint service that you want to manage.
4. On the details page of the endpoint service, click the **Endpoint Connections** tab, find the endpoint connection that you want to manage, and then click **Allow** in the **Actions** column.
5. In the **Allow Connection** dialog box, perform operations based on your business requirements:
   - If no service resource is available in the zone in which the endpoint is deployed, click **OK**.
   - If unallocated service resources are available in the zone in which the endpoint is deployed, click the check box for **Allow connections and automatically allocate service resources** and then click **OK**.

Modify the maximum bandwidth of an endpoint connection

The default maximum bandwidth of an endpoint connection is 1,024 Mbit/s. You can modify the maximum bandwidth based on your business requirements.

1. Log on to the Endpoint Service console.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, find and click the ID of the endpoint service that you want to manage.
4. On the details page of the endpoint service, click the **Endpoint Connections** tab, find the endpoint connection that you want to manage, and then click **Adjust Speed Limit** in the **Actions** column.
5. In the **Set Default Speed Limit** dialog box, specify a maximum bandwidth value and click **OK**.

   Valid values: **100 to 10240**. Unit: Mbit/s.

Reject endpoint connection requests

You can reject endpoint connection requests to an endpoint service. After you reject the connection request from an endpoint, you cannot use the endpoint to access the service resources of the endpoint service.

Before you reject an endpoint connection request, make sure that the following requirements are met:

1. The endpoint connection is in the **Connected** state.
2. The zone of the endpoint is in the **Connected** or **Disconnected** state.

After you reject an endpoint connection request, the status of the endpoint connection changes to **Rejected**.

1.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, find and click the ID of the endpoint service that you want to manage.
4. On the details page of the endpoint service, click the **Endpoint Connections** tab, find the endpoint that you want to manage, and then click **Deny** in the **Actions** column.
5. In the **Deny Connection** message, click **OK**.

References

- EnableVpcEndpointConnection: accepts the connection request from an endpoint.
- UpdateVpcEndpointConnectionAttribute: modifies the maximum bandwidth of an endpoint connection.
- DisableVpcEndpointConnection: rejects the connection request from an endpoint.

2.4.2. Modify the bandwidth of an endpoint connection

The default bandwidth of an endpoint connection is 1,024 Mbit/s. You can modify the bandwidth based on your business requirements.

Procedure

1. Log on to the Endpoints Service console.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, click the ID of the endpoint service.
4. On the **Endpoint Connections** tab, find the endpoint connection that you want to manage and click **Change Bandwidth** in the **Actions** column.
5. In the **Change Bandwidth** dialog box, specify the bandwidth based on your business requirements and click **OK**.

   Valid values: 100 to 1024. Unit: Mbit/s.

Related information

- UpdateVpcEndpointConnectionAttribute

2.4.3. Accept endpoint connection requests

This topic describes how to accept endpoint connection requests. If you have not set the endpoint service to automatically accept endpoint connection requests, you must manually accept endpoint connection requests. After you accept the connection request from an endpoint, the virtual private cloud (VPC) where the endpoint is deployed can use the endpoint to access an endpoint service that is deployed in another VPC.

Procedure

1.
2.
3. In the top navigation bar, select the region where the endpoint service is deployed.
4. On the **Endpoint Service** page, click the service ID of the endpoint service that you want to manage.
5. Click the **Endpoint Connections** tab, find the endpoint from which you want to accept requests, and then click **Allow** in the **Actions** column.
6. In the **Allow Connection** message that appears, click **OK**.

Related information

- EnableVpcEndpointConnection

2.4.4. Reject endpoint connection requests

This topic describes how to reject endpoint connection requests sent from endpoints. After you reject connection requests, the VPC where the endpoint is deployed cannot access the endpoint service.

Procedure

1.
2.
3. In the top navigation bar, select the region where the endpoint service is deployed.
4. On the **Endpoint Service** page, click the service ID of the endpoint service.
5. On the **Endpoint Connections** tab, find the endpoint from which you want to reject connection requests, and then click **Forbid** in the **Actions** column.
6. In the **Reject Connection** message, click **OK**.

Related information

- DisableVpcEndpointConnection

2.5. Manage the service whitelist

2.5.1. Manage account IDs in the whitelist

After an endpoint service is created, the ID of the Alibaba Cloud account of the service owner is automatically added to the whitelist. Users whose account IDs are in the whitelist can query the endpoint service and use endpoints to connect to the endpoint service. If you want to allow a virtual private cloud (VPC) that belongs to another Alibaba Cloud account to access the endpoint service, you must add the ID of the Alibaba Cloud account to the whitelist.

Operations

- Add account IDs to the whitelist
- Remove account IDs from the whitelist

Add account IDs to the whitelist

1. Log on to the Endpoint Service console.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, find and click the endpoint service that you want to manage.
4. On the details page of the endpoint service, click the **Service Whitelist** tab, and then click **Add to Whitelist**.
5. In the **Add to Whitelist** dialog box, enter the account IDs that you want to add to the whitelist, and then click **OK**.

   You can add one or more account IDs to the whitelist at a time. Separate account IDs with commas (,).

Remove account IDs from the whitelist

You can remove account IDs from the whitelist of an endpoint service. After an account ID is removed from the whitelist of an endpoint service, the account cannot query the endpoint service or use an endpoint to connect to the endpoint service.

1. Log on to the Endpoint Service console.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, find and click the endpoint service that you want to manage.
4. On the details page of the endpoint service, click the **Service Whitelist** tab, find the account that you want to remove, and then click **Delete** in the **Actions** column.
5. In the **Remove Account from Whitelist** message, click **OK**.

References

- AddUserToVpcEndpointService: adds an account ID to the whitelist of an endpoint service.
- RemoveUserFromVpcEndpointService: removes an account ID from the whitelist of an endpoint service.

2.5.2. Remove account IDs from the whitelist

This topic describes how to remove account IDs from the whitelist of an endpoint service. After an account ID is removed from the whitelist of an endpoint service, the endpoint service cannot be viewed under the account or accessed by endpoints under the account.

Procedure

1.

2.
3. In the top navigation bar, select the region where the endpoint service is deployed.
4. On the **Endpoint Service** page, find the endpoint service that you want to manage, and click the service ID of the endpoint service.
5. On the **Service Whitelist** tab, find the account ID that you want to remove from the whitelist, and click **Delete** in the **Actions** column.
6. In the message that appears, click **OK**.

Related information

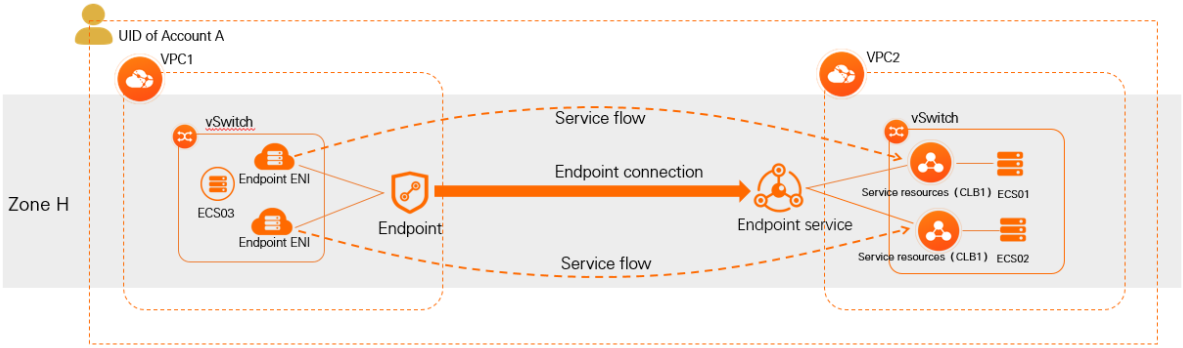
- RemoveUserFromVpcEndpointService

3.Manage service resources

PrivateLink allows you to specify instances as the service resources of endpoint services. When you accept the connection request from an endpoint to an endpoint service, you must allocate and connect a CLB instance to the endpoint elastic network interface (ENI) in the zone where the endpoint is created.

Scenarios

The following scenario is used as an example. A company created two virtual private clouds (VPCs) named VPC1 and VPC2 in Zone H of the China (Hangzhou) region with Account A. The two VPCs can communicate with each other over PrivateLink. Elastic Compute Service (ECS) instances are created in VPC2. Different NGINX services are deployed on the ECS instances. Two CLB instances named CLB1 and CLB2 are created in VPC2. Due to business development, the company wants to distribute some traffic from CLB1 to CLB2 to prevent overload on CLB1.



Limits

- The CLB instances that serve as service resources in VPC2 must be pay-as-you-go internal-facing CLB instances. Only pay-as-you-go internal-facing CLB instances support PrivateLink.
- The endpoint in VPC1, the endpoint service in VPC2, and the service resources in VPC2 must be deployed in the same zone of the same region.

Prerequisites

- VPC1 and VPC2 are created in the China (Hangzhou) region. A vSwitch is created in each VPC. For more information, see Create a VPC and a vSwitch.
- ECS03, which is used to send requests, is created in VPC1. ECS01 and ECS02, which are used to receive and process requests, are created in VPC2. Different NGINX services are deployed on ECS01 and ECS02. For more information, see Manually deploy an LNMP environment on an ECS instance that runs Alibaba Cloud Linux 2.
- CLB1 and CLB2, which serve as service resources, are created in VPC2. The CLB instances are deployed in Zone H. For more information about how to create a CLB instance that supports PrivateLink, see Create a CLB instance that supports PrivateLink.
- Listeners are created for CLB1 and CLB2. ECS01 is added as a backend server of CLB1, and ECS02 is added as a backend server of CLB2. For more information, see Configure a CLB instance.
- An endpoint is created in VPC1. An endpoint service is created in VPC2 and CLB1 in Zone H is specified as the service resource of the endpoint service. For more information about how to create an endpoint and an endpoint service, see Create an endpoint and an endpoint service.

The following table describes how to plan CIDR blocks for the VPCs. Make sure that the CIDR blocks do not overlap.

Attribute	VPC1	VPC2
Region	China (Hangzhou)	China (Hangzhou)
CIDR block	• VPC: 10.10.0.0/16 • vSwitch: 10.0.0.0/24	• VPC: 192.168.0.0/16 • vSwitch: 192.168.24.0/24
vSwitch zone	Zone H	Zone H
ECS instance IP address	ECS03: 10.0.0.190	• ECS01: 192.168.24.246 • ECS02: 10.0.0.189

Procedure

Step 1: Add a service resource to a zone

1.
2. In the top navigation bar, select the region to which the endpoint service in VPC2 belongs. In this example, **China (Hangzhou)** is selected.
3. On the **Endpoints Service** page, click the ID of the endpoint service that you want to manage.
4. On the **Service Resources** tab, click **Add Service Resource**.
5. In the **Add Service Resource** dialog box, select a zone to distribute traffic, and select the CLB instance that you want to associate with the endpoint service.

   In this example, **Hangzhou Zone H** and the ID of CLB2 are selected.
6. Click **OK**.

Step 2: Allocate and connect a service resource to a zone

Before you allocate and connect a service resource to a zone, make sure that the following requirements are met:

- The endpoint connection is in the **Disconnected** state.
- The zone of the endpoint is in the **Pending to Be Connected** or **Disconnected** state.
- A service resource is available in Zone H.

1. Click the **Endpoint Connections** tab, find the endpoint whose connection request you want to accept, and then click **Allow** in the **Actions** column.
2. In the **Allow Connection** dialog box, perform operations based on your business requirements:
   - If you want the system to automatically allocate service resources:

a. Select **Allow connections and automatically allocate service resources** and click **OK**.

b. Click the + icon next to the endpoint to show the zone details and select the zone that you want to manage. In this example, **Hangzhou Zone H** is selected.

c. Click **Connect to Service Resource** in the **Actions** column of the zone.

d. In the **Allow Connection** message, click **OK**.

- If you want to manually allocate service resources, clear the check box for **Allow connections and automatically allocate service resources**:

a. Click the + icon next to the endpoint to show the zone details and select the zone that you want to manage. In this example, **Hangzhou Zone H** is selected.

b. Click **Allocate Service Resource** in the **Actions** column of the zone.

c. In the **Allocate Service Resource** dialog box, click **Manual Allocation**, select CLB1, and then click **OK**.

> **Note** If a service resource exists in the zone of the endpoint and you select **Automatic Allocation**, the existing service resource is cleared. The service resource can be automatically allocated next time you select Allow connections and automatically allocate service resources for an endpoint connection.

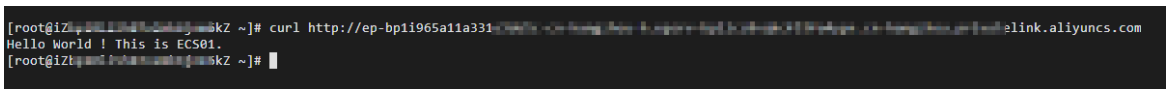
d. Click **Connect to Service Resource** in the **Actions** column of the zone.

e. In the **Allow Connection** message, click **OK**.

3. Log on to ECS03 and run the **curl** command to test whether ECS03 in VPC1 can access the service deployed on ECS01 in VPC2. For more information about how to log on to an ECS instance, see Connection methods.

```
curl https://<Domain name of the zone of the endpoint>
```

The following figure shows that ECS03 can access the service on ECS01.



Step 3: Create an alert rule

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, click **Cloud Service Monitoring**.
3. On the **Cloud Service Monitoring** page, click **PrivateLink** in the **Network** section.
4. On the **PrivateLink** page, click **Create Alert Rule** in the upper-right corner.
5. In the **Create Alert Rule** panel, set the following parameters and click **Confirm**:

   The following section describes the key parameters that are related to an endpoint service. For more information about the other parameters, see Create an alert rule.

   - **Product**: In this example, **PrivateLink** is selected.
   - **Resource Range**: Specify the application scope of the alert rule. In this example, **Instances** is selected.
   - **Associated Resources**: In this example, the endpoint service that is created in VPC2 is selected.

- **Rule Description**: Specify the content of the rule. An alert is triggered if the specified metric meets the specified condition.

  Click **Add Rule**. In the **Add Rule Description** panel, set the following parameters and click **OK**.

Parameter	Description
Alert Rule	Enter a name for the rule.
Metric Type	Select the type of the metric that is used to trigger an alert. In this example, **Single indicator** is selected.
Metric	Select a metric from the drop-down list. In this example, **Service Resource Inbound Bandwidth** is selected.
Please select dimension	Select the region and ID of the service resource. In this example, **cn-hangzhou-h** is selected for the **zoneId** parameter and the ID of CLB1 is selected for the **resourceId** parameter.
Threshold and Alert Level	Specify the threshold value of the metric and the severity level of the alert. In this example, **Warning Text Message + Email + DingTalk** is selected as the severity level and **1 Consecutive Cycles (1 Cycle = 1 Minutes) Average >= 100 Mbit/s** is specified as the alert condition. This specifies that the inbound bandwidth of the service resource is checked every minute. If the inbound bandwidth is equal to or greater than 100 Mbit/s once, an alert is triggered.
Chart Preview	Displays the monitoring chart of the metric in the specified period.

- Click **Advanced Settings** and set the following parameters:
  - **Mute for**: Specify the interval at which alert notifications are sent if the alert is not cleared. In this example, **30 min** is selected.
  - **Effective Time**: Specify the time period during which the alert rule remains effective. CloudMonitor checks monitoring data and determines whether to generate alerts only during the effective period. In this example, **00:00 - 23:59** is specified.
- **Alert Contact Group**: Specify the contact group to which alert notifications are sent. For more information about how to create a contact and a contact group, see Create an alert contact or alert contact group.

Step 4: Use wrk to perform a stress test

Use wrk to perform a stress test on the backend server of CLB1 (ECS01) in VPC2. When the inbound bandwidth of ECS01 reaches the specified threshold value, an alert is triggered in CloudMonitor.

> **Note** In this example, ECS03 runs the Alibaba Cloud Linux operating system. For more information about how to use the ping command in other operating systems, see the user guide of the operating system that you use.

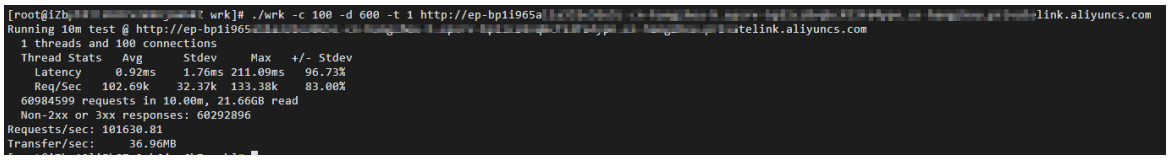
1. Log on to ECS03 in VPC1.
2. Run the following commands on ECS03 to install wrk:

```
yum -y install git make gcc
git clone https://github.com/wg/wrk.git
yum install unzip
cd wrk
make
```

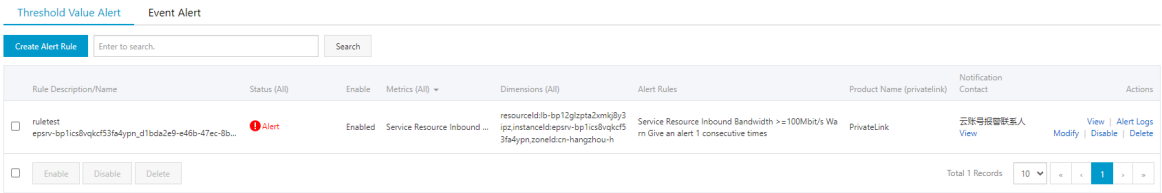
3. After wrk is installed, run the following command to perform a stress test on ECS01 by using wrk.

```
./wrk -c 100 -d 600 -t 1  http://<Domain name of the zone of the endpoint>
```

If the following echo reply packet is returned, the stress test is completed:



4. Return to the **Alert Rules** page in Step. After a few minutes, Alert is displayed in red in the Status column. This indicates that the inbound bandwidth of CLB1 reaches the threshold value. In this case, you can reduce the workload on CLB1 by distributing some traffic to CLB2.



Step 5: Replace a service resource in a zone

Before you replace a service resource, make sure that the following requirements are met:

- The endpoint connection is in the **Connected** state.
- The zone of the endpoint is in the **Connected** or **Disconnected** state.
- Other than CLB1, at least one service resource is available in Zone H.
- Automatic allocation is disabled for CLB1. For more information, see Enable and disable automatic allocation for a service resource.

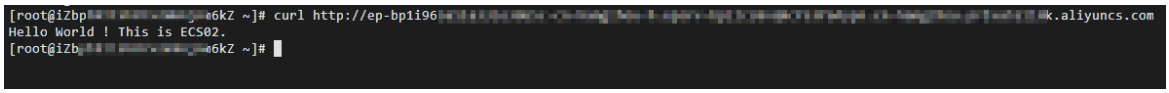
1.
2. In the top navigation bar, select the region where the endpoint service is deployed. In this example, **China (Hangzhou)** is selected.
3. On the **Endpoints Service** page, click the ID of the endpoint service that you want to manage.
4. On the endpoint service details page, click the **Endpoint Connections** tab, find the endpoint that you want to manage, and click the + icon next to the endpoint to show the zone details.
5. Select the zone that you want to manage and click **Replace Service Resource** in the **Actions**

column.

6. In the **Replace Service Resource** dialog box, click **Smooth Migration** or **Forcible Migration**, select CLB2, and then click **OK**.
7. After CLB1 is replaced, log on to ECS03 and run the **curl** command to test whether ECS03 in VPC1 can access the service deployed on ECS02 in VPC2.

   ```
   curl https://<Domain name of the zone of the endpoint>
   ```

   The following figure shows that ECS03 can access the service on ECS02.



What to do next

Enable and disable automatic allocation for a service resource

Before you can disable automatic allocation for a service resource, make sure that at least one service resource that can be automatically allocated is available in a zone.

1.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, click the ID of the endpoint service that you want to manage.
4. On the endpoint service details page, click the **Service Resources** tab, find the service resource that you want to manage, and turn on or turn off the switch in the **Automatic Allocation** column based on your business requirements.
   - Turn on the **Disabled** switch. In the **Do you want to enable automatic allocation?** message, click **Allow**.
   - Turn off the **Enabled** switch. In the **Are you sure that you want to disable automatic allocation?** message, click **Disable**.

Disconnect a service resource from a zone

Before you disconnect a service resource from a zone, make sure that the following requirements are met:

- The endpoint connection is in the **Connected** state.
- The zone of the endpoint is in the **Connected** state.
- A service resource is allocated to the zone of the endpoint.

1.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, click the ID of the endpoint service that you want to manage.
4. On the endpoint service details page, click the **Endpoint Connections** tab, find the endpoint that you want to manage, and click the + icon next to the endpoint to show the zone details.
5. Select the zone that you want to manage and click **Disconnect from Service Resource** in the **Actions** column based on the following scenarios:
   - In a smooth migration scenario, click **Disconnect from Previous Service Resource** and then click **Disconnect from Service Resource**.

- In a scenario in which a forcible migration is performed or no migration is performed, click **Disconnect from Service Resource**.

  > **Note**
  >
  > In a smooth migration scenario, the new endpoint ENI and the previous endpoint ENI must be displayed in the zone details.

6. In the **Are you sure that you want to disconnect from the service resources?** message, click **Yes**.

Delete a service resource

1.
2. In the top navigation bar, select the region where the endpoint service is deployed.
3. On the **Endpoints Service** page, click the ID of the endpoint service that you want to manage.
4. On the endpoint service details page, click the **Service Resources** tab, find the service resource that you want to delete, and perform operations based on the following scenarios:
   - If a service resource is not allocated to a zone of an endpoint:
     a. Find the service resource that you want to delete and click **Delete** in the **Actions** column.
     b. In the **Remove Resource** message, click **OK**.
   - If a service resource is allocated to a zone of an endpoint:
     a. Find the service resource that you want to delete and click **Replace Resource** in the **Actions** column.
     b. In the **Replace Service Resource** dialog box, set the following parameters and click **OK**.

Parameter	Description
Migration Type	Select **Smooth Migration** or **Forcible Migration** based on your business requirements. ■ If you select **Smooth Migration**, click **Release Previous Endpoint Connections** in the **Actions** after the migration is completed. After the previous connections are released, delete the service resource. ■ If you select **Forcible Migration**, you can directly delete the service resource after the migration is completed.
Select Destination Service Resource	Select the service resource that is used to replace the current service resource.
Select Source Endpoint Connection	Select the endpoint connection that is associated with the current service resource.

     c. Find the service resource that you want to delete and click **Delete** in the **Actions** column.

d. In the **Remove Resource** message, click **OK**.

> **Note** If the service resource that you want to delete is allocated to a zone of an endpoint, you must turn off the **Enabled** switch in the **Automatic Allocation** column of the service resource on the **Service Resources** tab.

References

- UpdateVpcEndpointZoneConnectionResourceAttribute: modifies the service resource of a zone to which an endpoint connection belongs.
- EnableVpcEndpointZoneConnection: accepts connection requests from an endpoint in a zone.
- DisableVpcEndpointZoneConnection: rejects connection requests from an endpoint in a zone.
- UpdateVpcEndpointServiceResourceAttribute: modifies a service resource of an endpoint service.
- DetachResourceFromVpcEndpointService: removes a service resource from an endpoint service.

4.Service linked role

This topic introduces the service linked role AliyunServiceRoleForPrivatelink for PrivateLink. You can delete the service linked role if you no longer need it.

Service linked role

Service linked roles are Resource Access Management (RAM) roles that can be assumed by linked Alibaba Cloud services. An Alibaba Cloud service may need to access other services to perform a specific function. Before you can access a service, make sure that authorization is granted for the service. Service linked roles simplify the authorization and avoid the risks caused by user errors. For more information, see Service-linked roles.

Create the service linked role for PrivateLink

When you create an endpoint, the system automatically creates a service linked role. The service linked role can delegate permissions to the endpoint and allows the endpoint to access other cloud resources. The service linked role that the system automatically created is AliyunServiceRoleForPrivatelink. After the service linked role is created, the system automatically attaches the AliyunServiceRolePolicyForPrivatelink policy to the service linked role. This way, permissions are granted to the service linked role and the endpoint can assume this role to access other cloud resources. The content of the policy is:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVSwitchAttributes"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:CreateNetworkInterface",
        "ecs:DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:CreateNetworkInterfacePermission",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:DeleteNetworkInterfacePermission"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "privatelink.aliyuncs.com"
        }
      }
    }
  ]
}
```

Delete the service linked role for PrivateLink

Before you delete the service linked role for PrivateLink (AliyunServiceRoleForPrivatelink), you must delete the endpoint to which the service linked role is assigned. For more information, see Delete an endpoint.